Case Study:
Management has decided to defer your upcoming SIS proof testing. Now what?

Mike Scott, PE, CFSE
aeShield
mike.scott@aeshield.com

Greg Swinson
aeShield
greg.swinson@aeshield.com

Keywords: Safety Instrumented Functions, Instrumented Safeguards, Proof Testing, IEC 61511, Management of Functional Safety, Risk, Risk Gaps

Abstract

Your boss walks into your office and states that plant management has decided to defer the upcoming planned shutdown for two years due to extremely high product demand. The specific question put to you is:

"The decision is final to extend the shutdown. What I need to know is what is our risk and what can we do to mitigate any potential increased risk knowing we've deferred Safety Instrumented System testing an additional 2 years?"

This white paper will walk through the typical steps / analysis one must complete to be able to answer this simple but complex question. This includes reviewing:

- Updated SIL Verification Calculations that include the new extended Test Interval
- Review the LOPA Target Risk Reduction Factor (RRF) versus Achieved RRF with the extended Test Interval to identify all Risk Gaps
- Review current performance status of these Safety Instrumented Functions (SIFs):
    - Are any of these functions already overdue for testing?
    - Are any of these functions being bypassed excessively?
    - Are any of the field devices used in these SIFs experiencing "high" failures?
    - Are any of these SIFs experiencing "high" demands?
- Review areas of potential high risk to identify any other potential compensating measures that could be implemented to mitigate / reduce risks

With this large compliment of data, the final challenge is how to communicate the potential increased risk to business in a way that management can readily understand and thus be empowered to make informed business decisions with regards to the various potential other compensating measures being recommended.

Introduction/background

In the process industry Safety Instrumented Systems play a critical role in protecting industrial processes and ensuring operational safety. Proof testing is one of the most important parts of ensuring the ongoing effectiveness and reliability of Safety Instrumented Systems.

Testing serves multiple purposes: it detects potential dangerous undetected failures, validates that the SIS can respond as designed, and confirms that the system's performance meets the required safety integrity level. By testing instruments and finding failures before a real-world demand occurs one is proactively removing risk from the business.

IEC 61511 contains numerous references mandating testing of SIFs due to the critical importance of this activity.

11.8.1 The design shall allow for testing of the SIS either end-to-end or in segments. Where the interval between scheduled process downtime is greater than the proof test interval, then on-line test facilities are required.

11.8.2 When on-line proof testing is required, test facilities shall be an integral part of the SIS design.

16.2.2 Operation and maintenance procedures shall be developed in accordance with the relevant safety planning and shall provide the following:

- *the information which needs to be maintained on SIS failure and the demand rates on the SIS;*
- *procedures for collecting data related to the demand rate and SIS reliability parameters;*
- *the information which needs to be maintained showing results of audits and tests on the SIS;*

16.2.9 Discrepancies between expected behaviour and actual behaviour of the SIS shall be analysed and, where necessary, modifications made such that the required safety is maintained. This shall include monitoring the following:

- *the demand rate on each SIF (see 5.2.5.3);*
- *the actions taken following a demand on the system;*
- *the failures and failure modes of equipment forming part of the SIS, including those identified during normal operation, inspection, testing or demand on a SIF;*
- *the cause of the demands;*
- *the cause and frequency of spurious trips;*
- *the failure of equipment forming part of any compensating measures.*

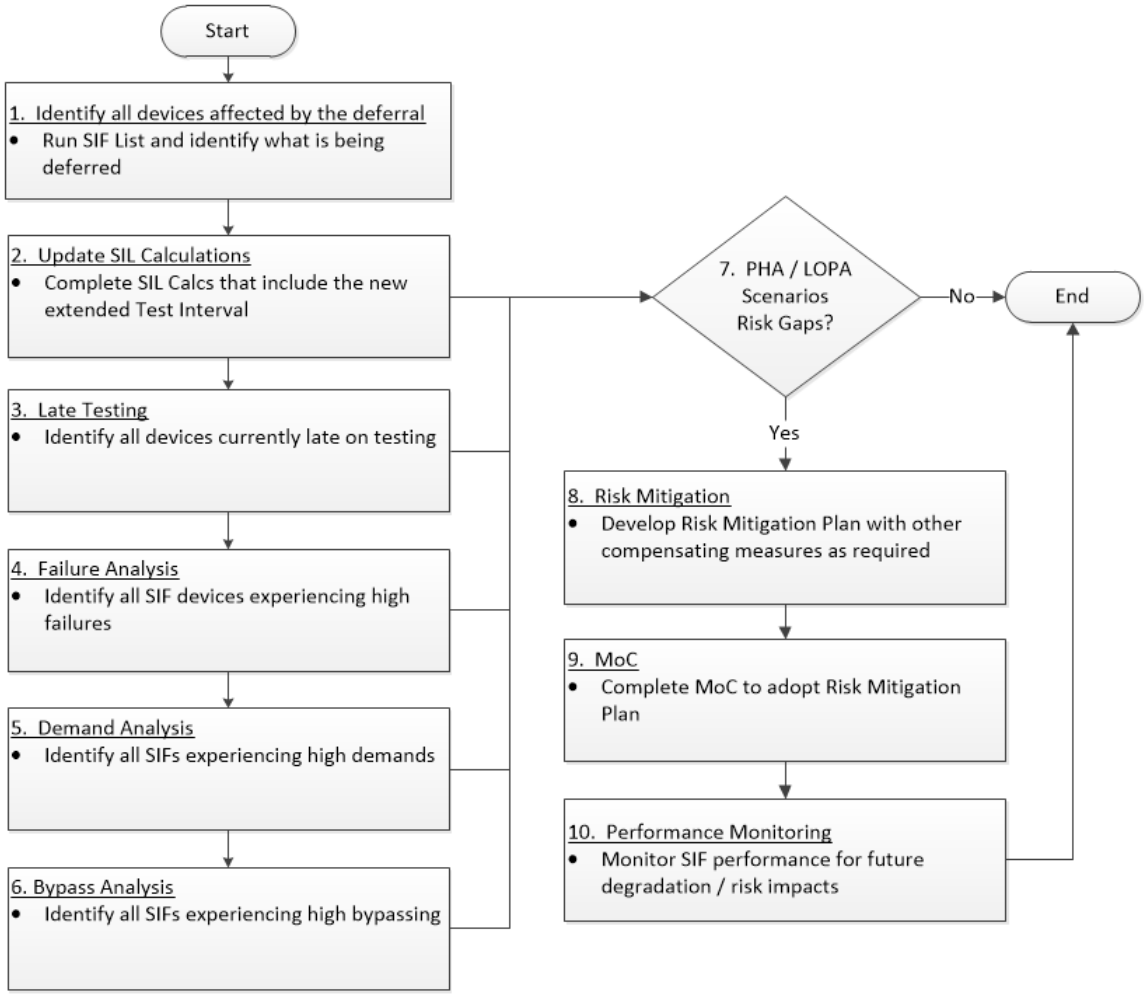
16.3.1.1 Periodic proof tests shall be conducted using a written procedure to reveal undetected faults that prevent the SIS from operating in accordance with the SRS.

This case study looks at a scenario where testing is deferred two years due to high production demand. One needs to evaluate the risk, identify any mitigation strategies, and communicate this to management and plant personnel.

Test Deferral Work Process

To identify all the tasks / steps that need to be considered a decision tree was created to communicate requirements more effectively to the personnel supporting this risk analysis effort and for the end users who would consume the resultant Risk Mitigation Plan. This work process was also documented such that it could be applied efficiently for similar events in the future. A simple ten (10) step approach as outlined in Figure 1 below was adopted.

Figure 1 – SIF Testing Deferral Decision Making Work Process



Each of these steps will be discussed in more detail in subsequent sections.

Step 1 - Identify all devices affected by the deferral

The first step is to identify all SIFs impacted by the new extended test interval. This requires one to compile a list of SIFs associated with process unit(s) included in the upcoming deferred Turnaround (TAR).

Figure 2 – Impact SIFs

Name	Description	PHA Reference	SIF Type	Target		Achieved			Inputs			Sensor Group Voting	Outputs			FE Group Voting	Logic Solvers	
				IL	RRF	IL	RRF	PFD	Tagname	Testing Interval (months)	Voting		Tagname	Testing Interval (months)	Voting		Logic Solver	Testing Interval (months)
SIF-1	Low Pressure SIF	Demo Node.02.1	SIF	1	100	2	120	8.30E-03	PT-1000A	12	1oo1	1oo1	XV-1001	12	1oo1	1oo1	AE-SPLC-001	60
SIF-2	High Pressure SIF	Demo Node.01.1	SIF	3	2,000	3	2,030	4.93E-04	PT-2000A PT-2000B	12	1oo2	1oo1	XV-2001 XV-2002	12	1oo2	1oo1	AE-SPLC-001	60
SIF-3	Low Flow SIF	Demo Node.08.1	SIF	1	100	2	210	4.75E-03	FT-3000A FT-3000B	12	1oo2	1oo1	XV-3001 XV-3002	12	1oo2	1oo1	AE-SPLC-001	60
SIF-4	High Flow SIF	Demo Node.07.1	SIF	1	100	2	194	5.14E-03	FT-4000A	12	1oo1	1oo1	XV-4001A XV-4001B	12	1oo2	1oo1	AE-SPLC-001	60
SIF-5	Low Temperature SIF	Demo Node.04.1	SIF	1	100	1	87	1.14E-02	TT-5000A	12	1oo1	1oo1	XV-5001A	12	1oo1	1oo1	AE-SPLC-001	60
SIF-6	High Temperature SIF	Demo Node.03.1	SIF	A	10	1	70	1.42E-02	TT-6000A	12	1oo1	1oo1	XV-6001	12	1oo1	1oo1	AE-SPLC-001	60
SIF-7	Low Level SIF	Demo Node.06.1	SIF	1	100	2	207	4.82E-03	LT-7000A	12	1oo1	1oo1	PM-7000A	12	1oo1	1oo1	AE-SPLC-001	60
SIF-8	High Level SIF	Demo Node.05.1	SIF	1	100	2	207	4.82E-03	LT-8000A	12	1oo1	1oo1	PM-7000B	12	1oo1	1oo1	AE-SPLC-001	60

Additionally, one needs review a SIF Gap report on the list above to see if there are current gaps. Thus, one needs to identify all SIFs that had legacy Risk Gaps prior to extending the proof test interval. As can be seen in Figure 3, one legacy Risk Gaps is present.

Figure 3 – SIF Gap Report

SIF Gaps: 1

SIF Name	Target IL	Target RRF	Achieved RRF	SIF Gap
SIF-5	1	100	87	13
SIF Description:	Low Temperature SIF			

Output of Step 1

- SIF List showing target vs achieved RRF with original test intervals
- SIF Gap Report flagging all legacy Risk Gaps

Step 2 – Update SIL Calculations

Once one has the list of SIFs and associated field devices, SIL Verification Calculations need to be updated to recalculate the achieved Risk Reduction Factor and Safety Integrity Level for the new extended test interval. Note if the initial assumed test interval was 1 year, the new extended test interval is now 3 years in total.

Comparing the target RRF set in the LOPA to the achieved RRF of the SIF allows one to evaluate the effectiveness of the safety system. If the SIF fails to meet the target, one classifies it as a Risk Gap and action needs to be taken to ensure risk can be maintained at an acceptable level. By extending the test interval of SIFs, one may be creating new Risk Gaps or increasing existing ones. Also, the SIF Gap report needs to be updated to include both legacy and new Risk Gaps. Figure 4 below shows three Risk Gaps have been identified

Figure 4 – Updated SIF Gap Report

SIF Gaps: 3

SIF Name	Target IL	New Achieved IL	Target RRF	Old Achieved RRF	New Achieved RRF	SIF Gap
SIF-2	3	2	2000	2030	907	1093
SIF Description:	High Pressure SIF					
SIF-5	1	1	100	87	29	71
SIF Description:	Low Temperature SIF					
SIF-4	1	1	100	194	90	10
SIF Description:	High Flow SIF					

NOTE: This is typically a manual approach of tracking down each SIF and changing the test interval in separate files and in multiple places within each SIL Calculation itself (sensors, logic solver, and final elements). One needs to also update SIF List and SIF Gap Report manually to reflect the new achieved RRFs / SILs.

Output of Step 2

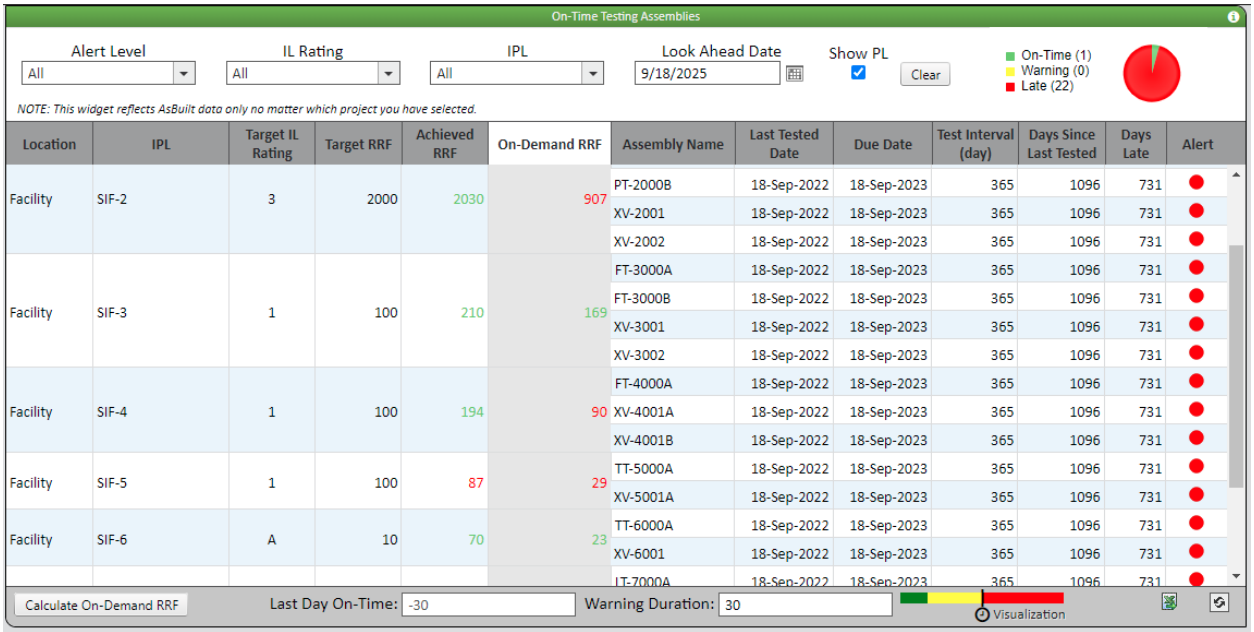
- Updated SIL Verification Calculations with new test intervals
- SIF List showing target vs achieved RRF with new test intervals
- SIF Gap Report flagging all Risk Gaps

Step 3 – Late Testing

The purpose of this step is to identify if any SIFs are currently overdue for testing. The new proposed test interval is now being extended to three (3) years assuming all SIFs were previously tested on time. So simplistically if existing SIFs were a year late to begin with, the testing deferral impacts would now extend SIF testing to four (4) years in total instead of three (3) years. This effort will also look at all field devices contained within all SIFs to ensure they have been tested and nothing has been "missed" (e.g., sensor was tested but, valve was not). All risk gaps should be flagged for an administrative MOC risk analysis. This will build on the list created when comparing LOPA RRF vs Updated Achieved RRF.

NOTE: This is typically a manual approach of tracking down each SIF within CMMS to confirm last tested date. If any late or missing testing was noted the SIL calculations must be manually updated. One needs to also update SIF List and SIF Gap Report manually to reflect the new achieved RRFs / SILs.

Figure 5 – Late Testing Impacts



Output of Step 3

- List of all SIFs and / or field devices currently with late or missing testing
- SIF List showing target vs achieved RRF with new test intervals
- SIF Gap Report flagging all Risk Gaps

Step 4 –Failure Analysis

The initial SIL Calculations have been completed with assumed failure rates for field devices. If actual performance is better or worse than these assumptions, one's Risk Gaps can be impacted in a positive or negative manner. So, this effort consists of reviewing SIF field device failures with the goal of making an informed decision on how testing deferral might impact future failures. Executing a proof test can positively impact SIF field device performance. For instance, if a pressure transmitter proof test plan includes a step to vent test pressure back into process piping to check for plugged taps, this step might also be "flushing" the taps. Therefore, excessively deferring testing in a fouling service might result in increased failures due to plugged taps. A similar concept exists for valves. A full stroke test of a valve could result in cleaning the valve seats of debris. Excessively deferring the full stroke of the valve could result in excessive debris build up such that the valve is unable to fully close / hold pressure. So a review of detailed examination of SIF field device performance records, maintenance logs, and historical data shall be performed to identify any devices have high failure counts and root causes of these failures.

Figure 6 – SIF Failure Counts

Failure Counts

Start: 2/15/2021 End: 9/18/2023 Include Systematic

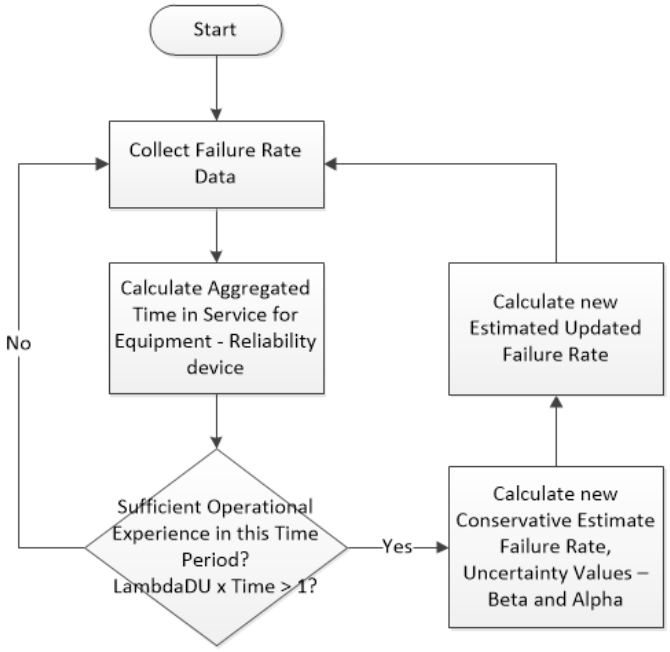
Location Tree	SD	SU	DD	DU	Total
ABC Petro Chemicals	1	1	2	3	7
Standards	1	1	2	3	7
North America	1	1	2	3	7
Plant 1	1	1	2	3	7
Unit 1	1	1	2	3	7
Plant 2	0	0	0	0	0

Figure 7 – Failure Classification Summary

Component	Equipment	Reliability	Manufacturer	Model	Service	Failure Date	Safe Detected	Safe Undetected	Dangerous Detected	Dangerous Undetected
XV-4001B	Generic ESD Valve	Generic Ball - Pneumatic Spring Return Actuator	Generic		Pneumatic	2023-03-16	FALSE	TRUE	FALSE	FALSE
FT-4000A	Generic Flow Transmitter	Generic DP or Gauge Transmitter	Generic		Gas	2023-04-12	FALSE	FALSE	TRUE	FALSE
XV-6001	Generic ESD Valve	Generic Ball - Pneumatic Spring Return Actuator	Generic		Pneumatic	2023-04-12	FALSE	FALSE	TRUE	FALSE
LT-8000A	Generic Level Transmitter	Generic DP or Gauge Transmitter	Generic		Gas	2022-11-29	FALSE	FALSE	FALSE	TRUE
TT-6000A	Generic Temperature Transmitter	Generic Temp Transmitter Excludes Element	Generic		Gas	2023-01-04	FALSE	FALSE	FALSE	TRUE
XV-3001	Generic ESD Valve	Generic Ball - Pneumatic Spring Return Actuator	Generic		Pneumatic	2023-02-06	FALSE	FALSE	FALSE	TRUE
PT-1000A	Generic Pressure Transmitter	Generic DP or Gauge Transmitter	Generic		Gas	2023-03-16	TRUE	FALSE	FALSE	FALSE

Upon review of failure data, a Prior Use Calculation can be updated if sufficient time has occurred. Refer to Figure 8 below for the recommended tasks / steps to review past failures and their impact on assumed failure rates. Details on Bayesian Prior Use Failure rate calculation is outside the scope of this current white paper but, will be documented in a future white paper by the authors.

Figure 8 – Prior Use Calculation Work Process



If a potential new failure rate for a SIF field device is warranted, new SIL Calculations should be completed showing impacts on achieved RRF for use of new Prior Use failure rate with current test interval and proposed new extended test interval. Increasing the test interval for SIFs associated with scenarios with excessive failures could create increased Risk Gaps. Conversely if Prior Use failure rates indicate better performance than initial assumptions, it might assist in Gap Closure associated with increased testing impacts to achieved RRF. All risk gaps should be flagged for an administrative MOC risk analysis. This will build on the list created when comparing LOPA RRF vs Updated Achieved RRF.

NOTE: This is typically a manual approach of tracking down each failure within CMMS with supporting failure classification details. SIL calculations must be manually updated for all potentially impacted SIFs. One needs to also update SIF List and SIF Gap Report to reflect the new achieved RRFs / SILs.

<u>Output of Step 4</u>

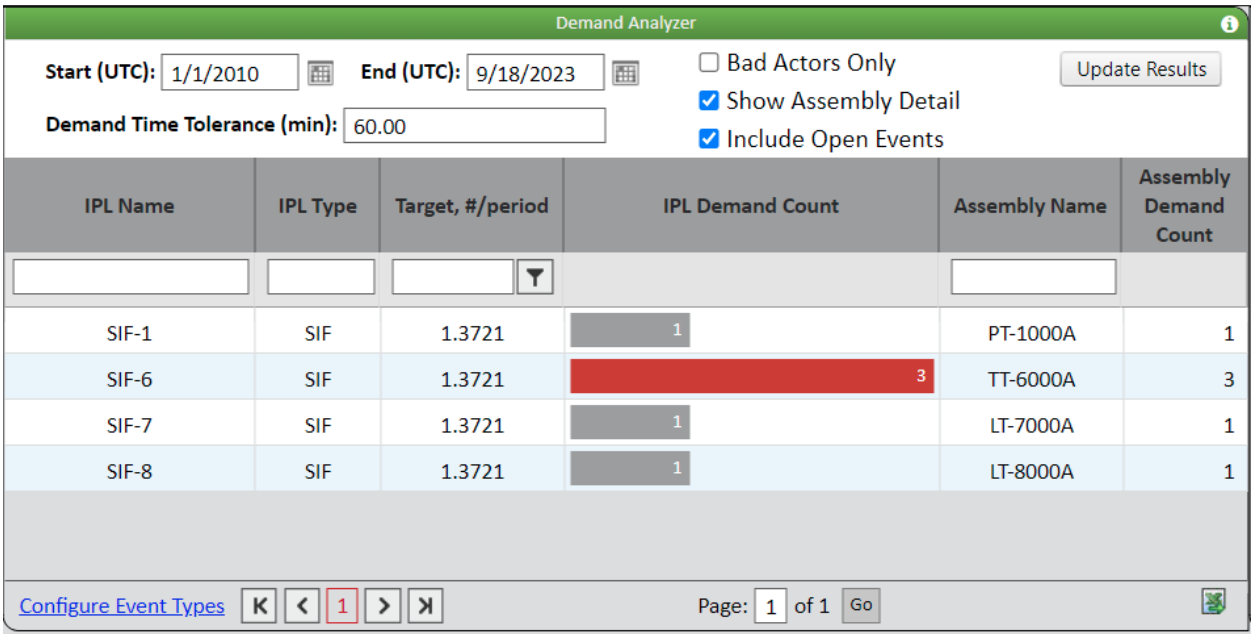
- SIF failure device counts from date of installation
- Failure Classification data of each failure
- Prior Use Failure Rate Calculation Update
- SIL Calculation Impact Analysis Report on potential new Prior Use Failure rates

Step 5 – Demand Analysis

Identifying SIFs with high demands will require looking at historical data, incident reports, and operational logs. Excessive demands could mandate an increase in the target RRF required for the SIF. This is critical as SIFs experiencing high demands should be evaluated to determine if the demands are causing a Risk Gap. If yes, then means need to be implemented to reduce the cause frequency, additional IPLs need to be identified and / or the SIF performance improved. Increasing the test interval for SIFs associated with scenarios with excessive demands could create increased Risk Gaps. All risk gaps should be flagged for an administrative MOC risk analysis. This will build on the list created when comparing LOPA RRF vs Updated Achieved RRF.

NOTE: This is typically a manual approach of tracking down each demand within the facility consolidated event journal, Sequence of Events log, historian, etc. with supporting demand classification details. LOPA causes must be manually updated to review potential RRF Target increases for SIFs in question. One needs to also update SIF List and SIF Gap Report manually to reflect the new achieved RRFs / SILs.

Figure 9 – Demand Counts



Output of Step 5

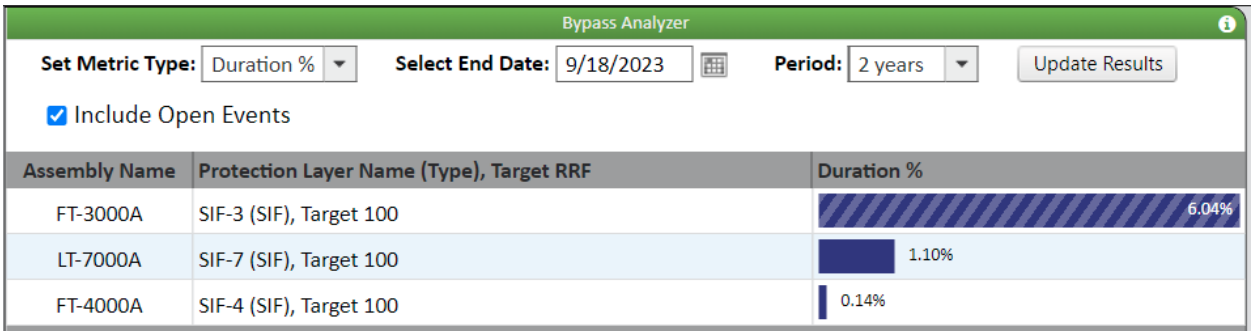
- Updated LOPA with new RRF targets
- SIF List showing target vs achieved RRF with new test intervals
- SIF Gap Report flagging all Risk Gaps

Step 6 – Bypass Analysis

Identifying SIFs with excessive time in bypass will require looking at historical data and / or bypass logs. This is critical as SIFs experiencing time in bypass should be evaluated to determine if the time in bypass is causing a Risk Gap. If yes, then reason for the bypass needs to be eliminated. This might require changes in design, additional IPLs need to be identified, and / or the SIF performance improved. Increasing the test interval for SIFs associated with scenarios with excessive time in bypass could create increased Risk Gaps. All risk gaps should be flagged for an administrative MOC risk analysis. This will build on the list created when comparing LOPA RRF vs Updated Achieved RRF.

NOTE: This is typically a manual approach of tracking down each bypass within bypass logs, the facility consolidated event journal, Sequence of Events log, historian, etc. with supporting bypass classification details. One needs to also update SIF List and SIF Gap Report to reflect the new achieved RRFs / SILs.

Figure 10 – Time in Bypass



Output of Step 6

- SIF Gap Report flagging all Risk Gaps

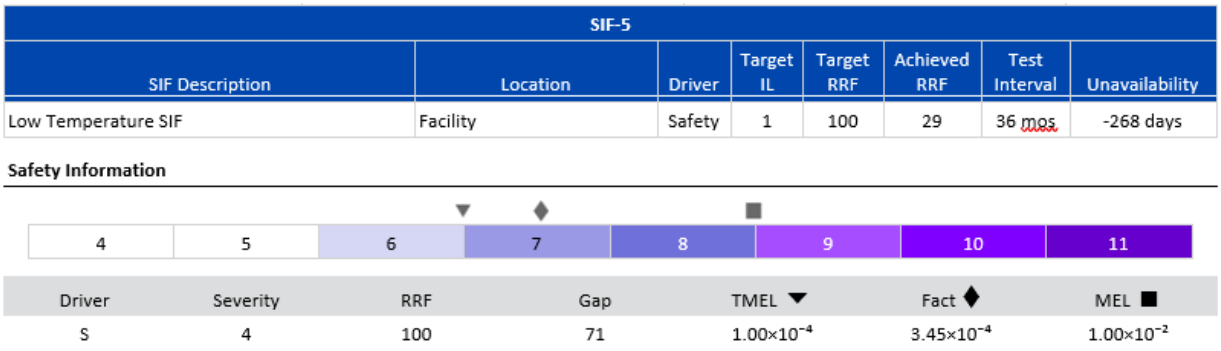
Step 7 – PHA / LOPA Review for Risk Gaps

With data in hand from Steps 1 to 6, PHA / LOPA scenarios should be updated to reflect revised reflect current Risk Ranking associated with testing deferral to include:

- Updated SIF PFDavg values reflecting extended Test Interval, Any Impacts to Current Late Testing, and / or Prior Use Failure Rates
- Updated Cause Frequencies
- Updated SIF Unavailable due to Bypassing

NOTE: This is typically a manual approach of updating SIF PFD_{avg} values in LOPA, updating cause frequencies, updating Bypass Impacts. One needs to also manually update the LOPA Gap Report.

Figure 11 – Risk Analysis



SIF-5							
SIF Description	Location	Driver	Target IL	Target RRF	Achieved RRF	Test Interval	Unavailability
Low Temperature SIF	Facility	Safety	1	100	29	36 mos	-268 days

Safety Information

4	5	6	7	8	9	10	11

Driver	Severity	RRF	Gap	TMEL ▼	Fact ♦	MEL ■
S	4	100	71	1.00×10^{-4}	3.45×10^{-4}	1.00×10^{-2}

Output of Step 7

- Updated PHA / LOPA reflecting current performance and future testing deferral impacts
- LOPA Gap Report flagging all Risk Gaps

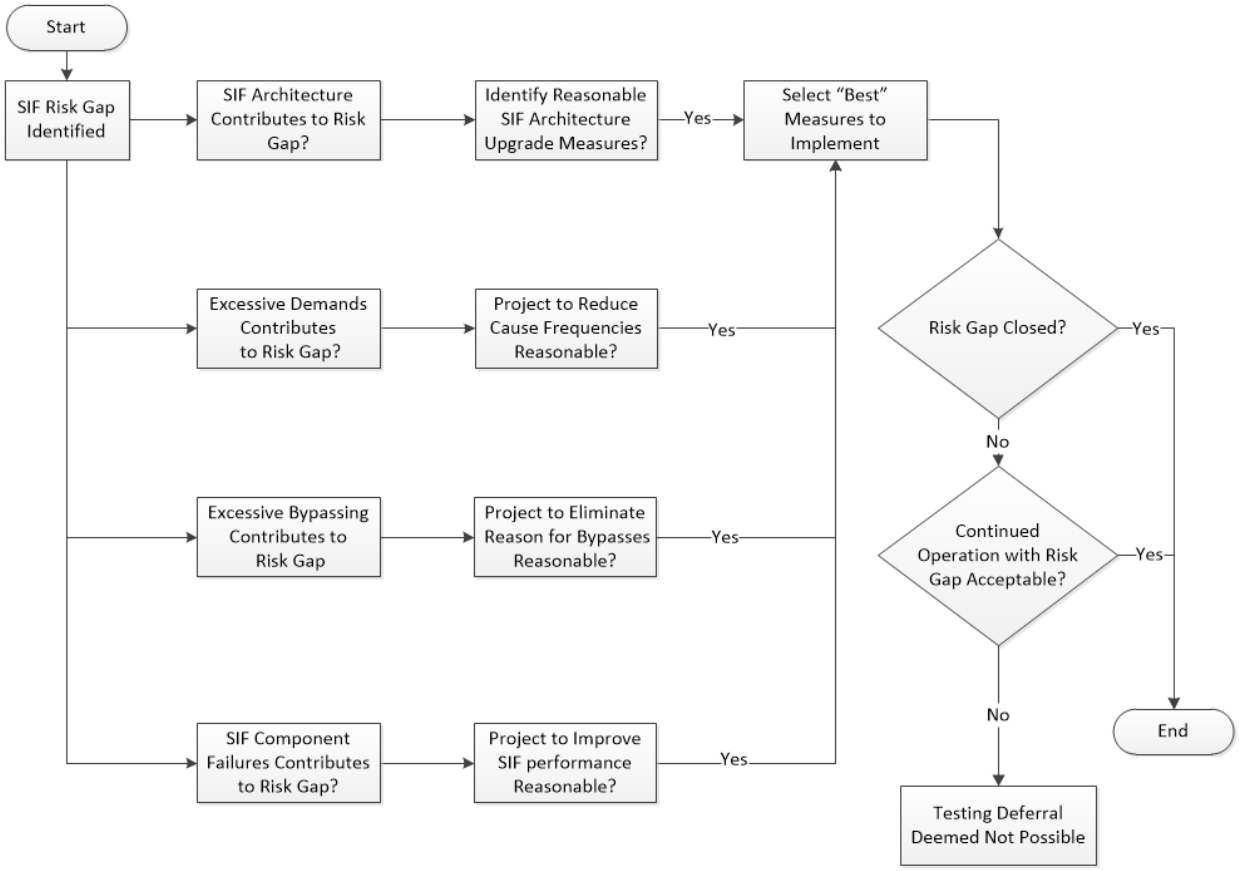
Step 8 – Risk Mitigation

All Risk Gaps identified in Step 7 need to be reviewed to determine:

1. If the Risk is going to be accepted as-is and business managed accordingly.
2. If other compensating measures are going to be implemented to reduce / manage risk.
3. Recommendations created and agreed upon for all requested modifications to manage risk.

To identify all the potential other compensating measures a decision tree was developed to communicate requirements more effectively to the personnel supporting this risk analysis effort and for the end users who would consume the resultant Risk Mitigation Plan. This work process was also documented such that it could be applied efficiently for similar events in the future. Figure 12 depicts the work process implemented.

Figure 12 – Identification of Other Compensating Measures



Engineering judgement and determination on "best" and / or reasonable risk reduction mechanisms was completed during a facilitated team meeting comprised of process / functional safety, operations, and maintenance. Factors considered included:

- Implementation mandates Production Outage or can be implemented Online
- Amount of Risk Reduction possible for the mechanism
- Effectiveness of the risk reduction mechanism to prevent the hazard in its entirety
- Cost of implementation

With consensus reached amongst the team, recommendations were created and documented in a Risk Mitigation Plan, which was subsequently issued for use.

Output of Step 8

- Risk Mitigation Plan

Step 9 – MoC

The agreed upon recommendations / actions identified in the Risk Mitigation Plan need to be implemented on site. These could be administrative changes and / or require capital project(s) with construction requirements. As such a MoC should be created to implement mandated actions contained in Risk Mitigation Plan.

Output of Step 9

- MoC to implement Risk Mitigation Plan recommendations

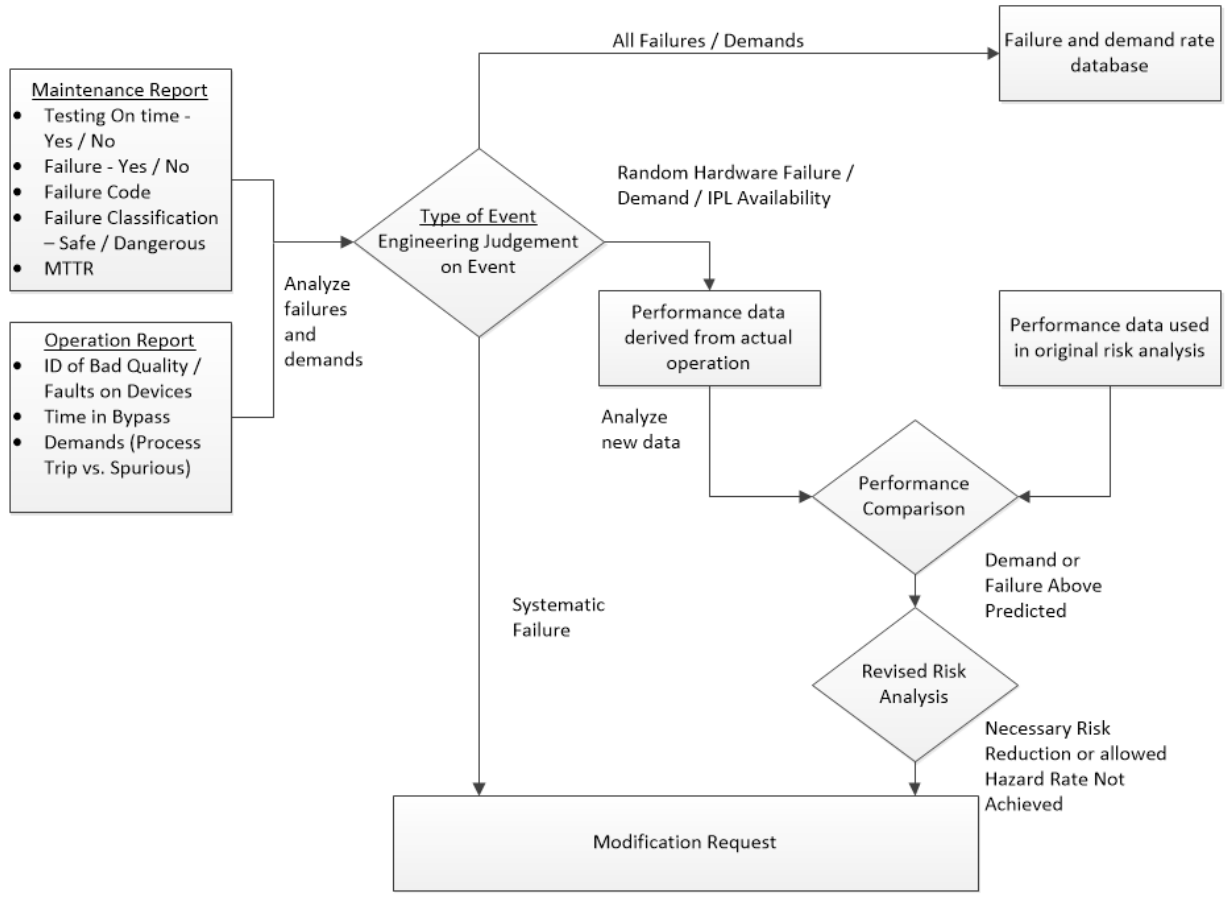
Step 10 – Performance Monitoring

As a continuous improvement activity SIF performance should be continued to be monitored in as an ongoing activity during the extended test interval and beyond. This should include:

- Late Testing
- Excessive Failures
- Excessive Demands
- Excessive Bypassing

Should any issues arise steps 3 – 9 shall be repeated to determine if any corrective actions are required. These requirements are key tenants to overall risk management as contained in both IEC 61508 and IEC 61511 and are depicted in Figure 13 below.

Figure 13 – Real time Monitoring of Risk



Output of Step 10

- Real-time Risk insight

Technology Enablement

As can be seen in each of the steps noted above, historically this has been a manual and very labour insensitive effort. As such most end users do not have the staffing / expertise onsite to be able to conduct a thorough review of Risk Impacts for Testing deferral as described above. However, new technology is available in the marketplace that enables end users to Digitally Transform the Data Collection, Risk Analysis, SIS engineering and IPL Bad Actor identification process such that all the above steps can be executed rapidly and efficiently. By enabling the end user to gain valuable insight into assumed versus actual Risk Ranking, informed business decisions can be made and communicated to plant personnel. Today's technology enables end users to effectively balance business needs / drivers around profitability while simultaneously ensuring high consequence process safety risks are effectively managed.

Conclusion

When proof testing is deferred it is critical to identify risk to the business and operational safety. Analysing updated SIL Calculations and current system performance will show risk gaps on the affected SIFs. A Risk Mitigation Plan can be documented detailing production impacts, amount of risk reduction possible, effectiveness of the risk reduction, and cost of implementation. A MOC should be created for all agreed upon recommendations and SIF performance should continue to be monitored.

Disclaimer

Although it is believed that the information in this paper is factual, no warranty or representation, expressed or implied, is made with respect to any or all of the content thereof, and no legal responsibility is assumed, therefore. The examples shown are simply for illustration, and, as such, do not necessarily represent any company's guidelines. The reader should use data, methodology, formulas, and guidelines that are appropriate for their own particular situation.

References

1. IEC 61508, Functional Safety of Electrical/Electronic/Programmable Safety-related Systems, Part 1-7, Geneva: International Electrotechnical Commission, 2010.
2. IEC 61511, Functional Safety: Safety Instrumented Systems for the Process Industry Sector, Parts 1-3, Geneva: International Electrotechnical Commission, 2017.